Norman

Workstation Configuration
Procedural Analysis
July, 1996

Computer Data Systems, Inc.
End User Systems Support Team
656 Quince Orchard Rd.
Gaithersburg, Md. 20878

Over time, the DOE Headquarters ASSIST (Automated Systems Security Incident Strike Team, formerly the CERT) has created a virus response process tailored to the DOE Headquarters environment to provide an optimal anti-viral program to combat what has escalated into a significant threat to DOE resources. Because the predominant anti-viral tool, DOEVStop, was developed in-house, this provided the luxury of designing it to fit the desired process. However, the conversion to a commercial off-the-shelf product may change this philosophy. The Norman Data Defense suite of products needs to be reviewed to determine how it can be applied to the DOE process or how the process must be adjusted to conform to the product. This paper provides an analysis of the Norman programs and their impact on the DOE anti-viral procedures.

NVC.SYS

The heart of any good anti-virus program is the use of a robust real-time monitor program. With the explosion of new viruses, a program that detects some significant number of unknown viruses is essential in the current environment. Norman's NVC.SYS is a resident, behavior blocking device driver that monitors activity and impedes behavior that is typical of viruses. It represents the cornerstone of the Norman suite and is essential to any implementation. However, while technically a superior product, its execution causes some conflicts with the existing response process, so a careful review of its functions is needed to identify the optimal configuration.

- **What options (parameters) in NVC.SYS should be activated?**

/A - Allow boot programs to pass

This mainly is used to prevent conflicts with other security programs, which should not be a factor in the DOE environment. This parameter should **not** be used. (There may be some factors concerning QEMM that need review.)

/B - Force the B) option (disable/clean and continue) from the list of user options.
/C - Disable option C) (ignore and continue) from the list of user options.

The three options presented in the event of a detection are:

A) reboot - The A) option may be severe, possibly resulting in loss of data, and it does not resolve the problem, producing a continual warning.

B) disable/clean and continue - In principle, this would be ideal. It allows the user to continue operations while awaiting ViRT response without the threat of possible propagation. However, if the infection is a boot sector virus on a diskette, B) erases the virus and then continues. Within the current response process, this is undesirable. Currently, most viruses attempt to enter DOE via diskette boot sectors. If the virus (which NVC.SYS does not report by name) is erased, the ViRT cannot determine if the virus is new and/or destructive. New viruses should be examined to determine their threat and ensure that proper eradication mechanisms are employed. Destructive viruses require a heightened response, especially to the media originator, which may have a serious problem. The ability to collect data and report by virus type also will be lost, making trend analysis difficult. To date, DOE's success at virus protection has been predicated on its data collection. In addition, when /B is used, **no** alert messages are displayed, with only an audio beep used to indicate that an abnormal event has occurred. Without sufficient displays, users will not know of the danger nor alert the proper parties, and this is considered a significant deficiency. Therefore, we recommend that the /B parameter **not** be used. Users then will have to be instructed on what to do in the event of an alert.

C) continue at your own risk - Obviously, this is a dangerous selection. However, if we are not comfortable with users selecting option B) in the event of a diskette boot sector infection, and option A) may be onerous, then C) may be the preferred course of action. Therefore, the /C parameter (which suppresses the C) option) should **not** be used. The viability of this direction will be dependent on the effectiveness of the incident notification function and may only be borne out from empirical results.

Norman Data Defense should be approached concerning alternatives to these options. Ideally, option B) would force a diskette removal rather than a clear, while providing appropriate informational messages. If this occurred, then using the /B parameter would be the preferred usage.

/D - Prevent direct access to the BIOS disk I/O functions.

Because this parameter precludes the use of 32-bit access in Windows, it should **not** be used. Previously, DOEVStop also had this problem, and there was sufficient negative user response that it was eliminated. It is likely that the scope of users' negative reactions will outweigh the minor benefits of using this option.

/F - Turn off file tracking

At Norman's direction, this mainly is needed in the event of false alarms. As no false alarms have occurred using NVC.SYS to date, there is no need to use this parameter.

/L - Disable logging to local hard drive
/N - No broadcast or logging on network

One of the attractive features of Norman's programs is their ability to log and report virus incidents. These should be activated as much as possible, so these options should **not** be used.

/M - Use monochrome

As monochrome monitors are passe, this parameter should only be needed on a special case basis.

/S - Suppress warning beep

Any feature that increases user awareness of potential dangers should be used, so beeps should **not** be suppressed.

/T - Disable virtual file testing on TSRs

This is one of NVC.SYS's algorithms for spotting unknown viruses and should be maintained. However, some programs (particularly memory managers) may cause false alarms. This parameter may be needed in isolated incidents, but should **not** be used in general.

Summary

In summary, NVC.SYS will be installed on the user workstations without **any** parameters. However, users will have to be educated **not** to select B) if a diskette-based virus is found (removing the diskette is preferred), but to use that option in all other cases. (This is not an ideal situation. Overtures should be made to Norman Data Defense for a design change.)

NVC.EXE

Virus scanners (i.e., programs that look for specific virus signatures) are and will remain an integral part of the virus protection process, especially in the areas of identification and eradication. When viruses first appeared, signature scanning algorithms were used as the primary mechanism for protection against computer viruses, providing both real-time monitoring and periodic hard disk and diskette checking. When the number of viruses was moderate, the time required to check for all virus signatures in a real-time mode was acceptable. Although the explosion of viruses has adversely impacted using scanning technology for real-time monitoring, pushing it to the edge of obsolescence, the need for precise virus identification for eradication and tracking still remains. In addition, scanning diskettes prior to use in a system is expected to continue to be an endorsed procedure. Thus, scanner technology will continue to be a strong asset in the overall strategy against computer viruses. In summary, even though scanner technology is not recommended for real-time monitoring, an *accurate* scanner that identifies the majority of known viruses is essential.

To address this need, Norman Virus Control provides one DOS-based program (NVC.EXE) that can be used with or without a menu-driven interface (ScanMenu) and one Windows-based program (NVCW.EXE).

- **What elements of NVC.EXE should be implemented?**

  At a minimum, the basic scanner, activatable from the DOS command line, should be included in any workstation implementation. Because an accurate scanner that identifies the majority of known viruses is critical and because the options can be controlled via batch files installed on user workstations, it is recommended that NVC.EXE be used at DOE.

  Norman provides two additional interfaces for improved user interaction:

  ScanMenu -

  > An alternative scanning mechanism is ScanMenu, which is the menu-driven DOS version of NVC.EXE. ScanMenu actually calls the NVC.EXE main program to facilitate the scanning, but it affords the user a menu-driven interface for selecting options. When scanning for viruses, the user may choose where to search (e.g., A: or C:, specific directories or files) and what areas to check (e.g., boot areas, all files) and what to do when a virus is found (e.g., report only, clean, or delete the file). Attempts were unsuccessful in providing a graying

mechanism for the delete and clean functions in ScanMenu through .INI files, functions which experience has shown should be relegated to ViRT staff only. As a result, ScanMenu is likely to cause difficulties or raise unnecessary questions. Because it provides no additional functionality and simple mechanisms for running the command line scanner can be implemented (just as they exist now with ResScan, without complaint), ScanMenu should **not** be a part of the workstation installation at DOE.

NVC for Windows -

In a Windows environment, users may want to use NVCW.EXE. It provides the same functionality and options offered by NVC.EXE, the DOS-based scanner. Since the Windows version uses a graphical user interface, it is inherently easier to use than the DOS command line counterpart. When the Windows version of Norman Virus Control is installed, three icons are present in the Norman program group: the Norman Virus Control icon that consists of the Windows Scanner, the Norman Windows Scanner Scheduler, and Norman's Virus Book.

The Windows program does give the user the option of deleting infecting files. This feature can be grayed out, however, by creating a file called NVC.MSG and inserting the appropriate commands to block out the option. This is possible via NVCW.EXE's built-in scripting language called Norman Control Script (NCS), providing the capability to customize the messages that NVCW.EXE displays, as well as other options. For example, the message that appears indicating that a possible virus has been found can be modified to include a message instructing the user to call the HOTLINE and any other specific information necessary. The script might also be helpful when NVCW.EXE is running from a network and all users should be using the same configuration of NVCW.EXE. Using NCS will override some of the settings contained within each individuals user's NVC.INI file, providing standardization.

Because there is a significant base of Windows users who may be more comfortable with that interface and the functions of the Windows scanner can be controlled, it is recommended that this module be included in the installation of Norman's product at DOE.

- **In what scenarios would the scanner be useful?**

The current workstation and response configuration also employs a basic scanning program, and there seems to be no reason that the new scanner cannot simply replace the old one in each case. This leads to four potential usages:

1) **Diskette scanning -** Users can scan diskettes from their systems. This is provided through an easy-to-use batch file called SCANA.BAT. It prompts users for multiple diskettes and only scans the directly affected system areas (the diskette itself).

2) **System scanning -** While in principle a system should never need to be scanned once a monitor is in place, some users nevertheless wish to scan their hard drives, and this may actually be valid in instances where the monitor and scanner address different virus universes (as the non-signature-based NVC.SYS and NVC.EXE do). Again, this can be easily implemented through a simple batch file (SCAN.BAT).

3) **Pre-installation scanning -** Before installing anti-virus software on a system, it is essential to ensure that it is virus-free beforehand. A basic scan of the computer is easily implemented into the installation process.

4) **Eradication-** The scanner is the main component for virus removal, as it can definitively identify the virus strain and then perform the appropriate tailored removal. Therefore, the scanner will be the heart of the response mechanism. This scenario is not addressed in this paper.

- **What command line options (parameters) should be used?**

The following is a list of parameters available for use with the DOS scanner. A brief description follows each parameter.

- /AD Scan all fixed drives.

  Since this option scans not only local drives, but also all available network drives if a user is logged on at the time the scanner is run, it should **not** be used. Servers will be protected through other means, and users should not be performing this function.

- /AF Scan all files.

The default file extensions that the scanner looks for without this parameter cover most infection possibilities. To scan all files rather than those at risk would increase scanning time dramatically. However, macro viruses contained in data files may not be detected if /AF is omitted. Because of the severe performance cost of activating this parameter, it will not be used in the initial implementation. However, the usage of this parameter may need to be reviewed at a later date based on the empirical results relating to macro virus protection.

- /ALD Scan all local drives (diskette drives are not scanned).

  This option will be used as a part of the SCAN.BAT file, which focuses on hard drive examinations. Diskette drives will be scanned using SCANA.BAT.

- /AM Scan for all resident viruses.

  Without this parameter, the scanner will search only for what Norman determines to be the "most dangerous viruses". Because scanning for all viruses in memory does not increase scan time significantly, it is recommended that the parameter be used.

- /B Turn off beep.

  It is our opinion that any audible means of informing a user of a virus infection is beneficial, so this option will not be used.

- /BS- Skip system area check.

  System areas should always be checked for added protection. Therefore, this option will not be used.

- /C Scan archive files.

  This option is not necessary, since the scanner can detect viruses contained within compressed files. However, eradication cannot be performed on these files without this parameter. Since eradication will not be done at the user level, this option is not necessary at the desktop, although it may apply for the eradication diskette.

- /CL Clean infected files.

  In general, allowing users to clean their own viruses undermines the Headquarters anti-viral response process, which is dependent on investigations to ensure containment for **all** users, not just the current user. Users who clear their own viruses usually do not notify the HOTLINE or perform a self-investigation, so the virus may continue to spread from the originator. To prevent this and ensure some form of response, /CL should **not** be activated. (Note that it will not function correctly without Norman's NVCLEAN module, which will not be provided to users in any case.)

- /D Delete and wipe infected files.
- /D- Delete infected files.

  This parameter deletes (and overwrites with /D) infected files. User access to this option would be detrimental to the ViRT's investigative function of finding virus sources and containing them. This parameter is not necessary for ViRT members either, since NVCLEAN.EXE will be used for eradication purposes.

- /E User-defined extensions.

  Up to three file extensions in addition to those scanned by default can be used. This is not necessary at this time, but may be useful in the future as virus technology increases and other file extensions become targets.

- /LA Log all scanned files.

  The logging of all scanned files rather than just the infected ones is not necessary. Therefore, this selection will not be used with the scanner.

- /LC List Norman system configuration.

  A list of all Norman programs installed is displayed with this parameter. This may be useful in the future by ViRT members, but is not necessary at the user level.

- /LG Append to log file.

  Results of scans are logged to a file that resides at the workstation. If this parameter is chosen, a running list of scan results is stored in the log file. At this time, the benefits of retaining historical scan data are nebulous, so this option will not be used.

- /LP Log to printer.

  The results of a scan can be sent to a printer using this parameter. Printing the results would not aid in eradication and would be an unwarranted use of paper.

- /LS Use short log file.

  A log file that contains the names of infected files only is written. See /LG above.

- /LV List virus library.

  A list of the viruses that Norman's product recognizes can be displayed. End users have no need for this information.

- /N Skip memory test.

  This parameter will be used as a part of the SCANA.BAT file to accelerate the scanning process, but will not be used with SCAN.BAT so that a full system review is performed.

- /O Skip open files.

  If this selection is not chosen, the scanner will stop when it reaches an open file, which is not desirable. With the option chosen, the scanner continues and makes a note in the log file as to which files were open and subsequently skipped during the scan. Consequently, this parameter will be used in both batch files.

- /Q Set quiet mode.

  No screen display is shown during the scan with this option. It is always a good idea to display scanning operations. Therefore, this parameter will not be used.

- /R Repeated scan of diskettes.

  Because the existing SCANA.BAT file already prompts for additional diskettes in a user-friendly manner, this option will not be used.

- /S Scan subdirectories.

  A scan of subdirectories is always desirable and will be used with both batch files. However, because full disk scans (as will be used in the basic batch files) automatically check all directories, this parameter can be omitted.

- /SN Inhibit user break.

  This parameter can be used to prevent a user from breaking out of a scan by pressing [Esc] or [Ctrl]+[Break]. This option is too restricting, since situations often occur where immediate access to the workstation is necessary. Restricting a user's ability to break out of a scan may result in their not wanting to use the scanner at all. Therefore, this parameter will not be used.

- /TEST Simulate virus detection.

  Although this parameter is useful to ASSIST personnel with testing of the product, a user would never have an occasion to use this, so it will not be provided.

- /UN Unattended mode.

  With this parameter set, the scanner will not stop and wait for user input to continue when it finds an infected file. Since it is preferable that the user see all warnings, this option will not be used.

- /X Look for EXE headers.

  Some sophisticated viruses store lists of .EXE files to infect. This parameter looks for those lists. However, because this affects scanning time and no such viruses have arisen at Headquarters, this parameter will not be used at this time.

- /Y Report variants by name.

  At the user level, having an exact identification is unnecessary, so this parameter will not be used for SCAN and SCANA. However, for investigative reasons, this would be helpful during response.

- /YH Stop at first virus found.

  In general, users and ViRT staff need to identify **all** viruses on a system, so the scan should not be stopped.

Summary

following DOS scanner configurations:

1) **Diskette scanning (SCANA) -**

   NVC.EXE /AM /N /O

   This will scan diskettes only without performing a memory scan, but checking for the full list of viruses.

2) **Disk scanning -**

   NVC.EXE /ALD /AM /O

   This will scan systems, checking all hard drives (and memory) for the full list of viruses.

3) **Pre-installation scanning -**

   NVC.EXE /ALD /AM /O

   This is the same configuration used for system scanning. No additional functionality is necessary.

NVCTSR

NVCTSR is a basic signature-checking monitor program.

- **Should NVCTSR be implemented?**

  NVCTSR's advantage over NVC.SYS is that it can identify and report viruses by name. Its disadvantages are that it does not detect unknown viruses, requires more maintenance to keep the signature database up to date, uses significantly more memory, and slows down system and network performance.

  Testing using NVCTSR produced an unacceptable degree of system degradation while using both local and network drives (although network performance by far was more severely affected). Because the negative effects of NVCTSR are obvious, users quickly would become agitated should the module be a part of the DOE installation of the Norman product suite. Further, because the amount of memory that it uses while running depends on the number of virus signatures it employs to detect viruses, its memory use will only increase as upgrades to the module are released and installed.

Norman's documentation states that NVC.SYS and an on-demand scanner, along with Canary, provide adequate protection against both known and unknown viruses. In addition, they do not use an exorbitant amount of memory. To use NVCTSR in addition to these modules is unnecessary and excessive.

Summary

In summary, since NVCTSR alters performance, may cause memory problems, and is not essential for virus protection given the other modules recommended for installation, NVCTSR should **not** be used.

BootGuard

BootGuard stores an image of the uninfected Master Boot Record of each machine and, when run, compares this image against the current Master Boot Record information.

- **Should BootGuard be implemented?**

If BootGuard detects a boot sector alteration, it displays a warning that the boot area was changed and offers the user three options:

(A) Save new boot area;
(B) Restore previous boot area;
(C) Ignore and Exit.

It then displays a message that users should choose "B" to restore the old boot files if they are not sure about the changes. If a user made a legitimate change to the Master Boot Record (for example, DOS was upgraded) and chose option "B" when BootGuard displayed its message, the original Master Boot Record would be restored, causing errors. (In this example, DOS command interpreter errors would result). If a virus does in fact exist, choosing option "A" would allow the virus-infected boot sector to be saved. Option "C" should **not** be chosen under any circumstances, as this may allow a virus to spread.

According to Norman, BootGuard may catch viruses that NVC.SYS may miss on boot-up. However, during our testing, NVC.SYS detected all viruses from the DOE library. Should BootGuard be a part of the DOE installation, each case would have to be looked at independently by qualified support staff to determine which option should be chosen for each incident. In a case where the user did not solicit help, he could potentially do more harm than good.

Summary

Since NVC.SYS provides adequate protection and because the likelihood that BootGuard would detect a virus not caught by NVC.SYS is considered minute, it is recommended that BootGuard **not** be included in the DOE installation of Norman's product.

Canary

Canary is a dummy program that should become infected if a file infector virus is active, thus allowing Norman to spot potential unknown viruses. It is non-resident and is not dependent on other modules of the Norman product. Two DOS programs (CANARY.COM and CANARY.EXE) are incorporated into the Canary module. When either becomes infected, an error message (or ErrorLevel, depending upon its setup) will appear indicating that either or both files have been altered. Canary does not detect the virus by name; therefore, one of the scanner modules should be used once Canary issues a message.

- **Should Canary be implemented?**

  Because Canary messages can be an early warning sign to file infector viruses and do not have any disadvantages with regard to other Norman modules or system usage, it is recommended that Canary be a part of the installation of Norman's Anti-Virus suite.

Binder

Binder (BD.EXE) is an integrity checker that is able to restore corrupted executable files, even without specific knowledge of the causal virus. It creates a database of integrity data for each .EXE file. Each directory then contains a hidden file called FILELOG.DAT.

- **Should Binder be implemented?**

  There are several disadvantages to using Binder. First, Binder provides on demand protection, rather than real-time. Therefore, user intervention is necessary for its use unless it was loaded through the AUTOEXEC.BAT file. As much as possible, virus protection should be automated and not user-dependant.

Second, the time that it takes for Binder to check all of the executable files when run is lengthy. Unless Binder were set up to run infrequently (which defeats its purpose), it would be more of a nuisance to the end user than a benefit. Because the program takes a considerable amount of time to run, users would be hesitant to use the program. If they were to run the program several times daily, it would result in an ineffective use of resources (lost time while waiting) that is not necessary given the other Norman products that will be used to handle the virus threat.

Third and most importantly, when a new file exists, the user is given the following message:

File is new. (D)elete, C(o)ntinue, E(x)it?

The user's may or may not know which option to choose. If a user were to choose the wrong option for the circumstances, ramifications would occur that would necessitate the need for support personnel to intervene, again causing an ineffective use of resources.

It is our belief that the time necessary to initialize and maintain the integrity database outweighs the benefit of using the module. Binder subsequently allows users to clear viruses without the need for ViRT response and potentially without review and investigation, a capability that should not be provided at the user level under the anti-virus protection plan at Headquarters.

Summary

In summary, because of a significant number of concerns, Binder is **not** recommended for use at DOE. Note that Binder, when used with NVCTSR, causes degradation in system performance.

Macro Viruses

Macro viruses in general, as typified by the Word Prank virus in particular, represent a new virus technology that has proved to be a challenge to anti-virus experts. Because the mechanism uses legitimate programming functions, macro viruses, especially unknown varieties, are difficult to identify. Because Norman focuses on behavioral blocking rather than signature checking, it likely will have a particularly difficult effort incorporating appropriate anti-viral measures in its product.

- **Can Norman detect macro viruses?**

  At this time, neither Norman monitor module (NVC.SYS nor NVCTSR.EXE) can detect any macro viruses. Because of NVC.SYS's behavioral algorithm, this is not unexpected. NVCTSR's failure is more surprising, since it relies on signature scanning technology, and viable signatures for these viruses have been identified (and are already in use at DOE Headquarters).

  The NVC.EXE scanner can detect macro viruses, although it does not provide removal capability. However, because macro viruses infect data files that can have **any** name and NVC.EXE by default only checks files with an extension of .DOC, infected files may not missed. The scanner can be directed to scan all files, but this incurs a substantial performance penalty (a scan can take a half hour or more) that is considered onerous at this time.

  To fill the gap, Norman does provides a Word Macro Virus Scanner (which runs only within Microsoft Word) that can scan files to eradicate the virus, clear the automated propagation mechanism, and remain active during Word sessions to detect future incursions.

- **Should the Norman Macro Virus Scanner be implemented?**

  The Norman Macro Virus Scanner appears to be a derivative of Microsoft's program. Currently, the ViRT utilizes the Microsoft- supplied scanning program to verify the existence of a macro virus and to remove the virus. When the ViRT completes the removal of the macro virus, it leaves the Microsoft program in place to inoculate the system from future infections. While the Norman product superficially appears to work in a similar manner, it has some deficiencies. In particular, it does not provide flexibility in selecting files to scan; it only checks files with .DOC and .DOT extensions (the default Word conventions). However, there is no requirement that users follow this convention (and many will not), so certain infected files may not be addressed.

Because the Norman solution closely mirrors the Microsoft solution, it is important to note that the deficiencies in the Microsoft Macro Virus Scanner are also inherent in the Norman Macro Virus Scanner. More specifically, while the Norman product can detect, remove, and inoculate the system from the macro viruses, it only works while the user is running the Word program. There is no other real-time monitoring mechanism provided by Norman that can detect these viruses outside of Word. In addition, the Norman Macro Virus Scanner provides very few informational messages and does not interact with Norman's automated server incident notification mechanism, so ViRT notification is likely to be omitted, further impeding the potential for investigative containment. Given the ViRT's focus on virus containment and resource protection, it is considered essential that real-time detection be available to identify the virus in e-mail or before conversions to other formats (such as WordPerfect, which inherently destroys the viruses). While the receiving user may not become infected or be in danger, failure to identify the existence of the virus and determine the source prevents assistive notification or response to the originating user, who will remain infected, potentially jeopardizing other users and resources.

Summary

Because the Microsoft macro virus scanner appears to provide superior functionality over the Norman version, it will continue to be used to address Word Prank macro virus incidents, as it does now. Because the macro scanner module is independent of all other components, this is acceptable, at least at this time.

- **What additional protections against macro viruses can be implemented outside of the Norman programs?**

While the Macro Virus Scanner provides protection for an individual workstation, it provides minimal aid in identifying potential sources and containing the spread, especially in this environment where Word is not widely used. A real-time monitoring mechanism for macro viruses, which Norman does not provide, is essential to prevent the spread of these viruses. The threat of these viruses is heightened, because they are the first to use data files as hosts. Since data files are often attached to e-mail messages, the macro viruses have proved to be very prolific.

To date, DOEVStop has provided real-time protection against these viruses.

Since an established mechanism exists for this class of virus, it is reasonable to simply continue its implementation. Therefore, while a significant subset of DOEVStop will be superseded by Norman, a pared down version focused on macro viruses can be maintained.

Fortunately, it appears this can be accomplished with minimal impact. A skeletal version of DOEVStop (renamed DOEVMon) would require only 1K bytes of memory. DOEVMon would continue to alert the user immediately if an infected data file is opened or copied. NVC.SYS does not recognize the virus in cc:Mail or when it is opened or copied.

Should DOEVMon not be used to augment the Macro Virus Scanner, macro viruses would not be detected unless the user opened the file in Word or regular scans were performed on **all** files. Once the macro scanner is installed in Word, any future infections would be cleaned automatically without the ViRT's knowledge. With DOEVMon active, tracking macro viruses would still occur, a critical element to keep viruses from spreading to potentially unprotected media. Although the macro viruses detected at DOE Headquarters are not destructive, it is only a matter of time until a dangerous one appears. It is imperative that investigations be performed to minimize the spread of viruses.

In addition, there are numerous logistical problems to relying on the Word Macro Virus Scanner. It must be loaded manually on each system that has Word, unlike the other programs in the suite that can be installed automatically and transparently from the LAN. Updated versions with new signatures will need to be installed periodically. In addition, macro viruses for other packages are appearing, eventually leading to a proliferation of anti-viral macros for each product. Maintaining the full library soon will become untenable. The use of macros to combat macro viruses should be considered a short-term solution. DOEVMon has more long-term potential as a preventative mechanism.

Summary

Since testing has shown that DOEVMon and NVC.SYS can co-exist, it is recommended that DOEVMon be instituted with the Norman product suite until Norman Data Defense releases a viable real-time TSR to address macro viruses.

Summary

In summary, the user workstation implementation will be as follows:

- The following modules will not be used:

  - **NVCTSR** - because it severely affects system performance, uses excessive memory, requires increased logistical support, and provides little additional benefits over NVC.SYS.

  - **BootGuard**- because it provides minimal additional capabilities while potentially increasing support requirements.

  - **Binder**- because its maintenance will impact user productivity, system performance may be adversely affected, and users can use it to circumvent desirable response processes.

- NVC.SYS will be the real-time monitor. It will be loaded in the CONFIG.SYS without any parameters. There are concerns about the options presented to the user when a virus is detected. These will need to be addressed initially through user education, with discussions undertaken with Norman for future alterations to their programs.

  For real-time monitoring for macro viruses, which Norman does not provide at this time, the Headquarters ASSIST will maintain DOEVMon, a skeleton version of its predecessor, DOEVStop.

- The NVC.EXE scanner program will be provided. Batch files to simplify diskette (SCANA) and system (SCAN) scanning will be implemented, as now. The Windows scanner module also will be provided for users who prefer that interface. ScanMenu, the graphical DOS interface to the scanner, will not be provided, as it has some bugs and provides some functions that users may misuse.

  Prompts for weekly scans will continue to be incorporated in the AUTOEXEC.BAT file, as they are now. In nearly all ways, the Norman scanner can simply be dropped in place of the existing scanner (ResScan) in all existing processes.

  Note that, in accordance with prior Headquarters protection procedures, the NVCLEAN eradication module will **not** be provided to users to ensure that virus incidents are properly reported and investigated.

- The Canary program for assisting in the detection of unknown file infector programs will be included in the AUTOEXEC.BAT file, as it can be implemented innocuously with potential benefit.

- The Norman Macro Virus Scanner will **not** be used because of limitations in the program. The Microsoft version will continue to be supplied to MS Word users.

There are several significant deficiencies with Norman as it applies to the DOE Headquarters anti-virus program. The first is NVC.SYS's handling of boot sector viruses on diskettes, where the user has the option of simply overwriting the virus. Users then may not report the incident (allowing the originator to unknowingly continue spreading the virus), and it will be impossible to determine the threat of the virus or if a new virus has entered the environment, both critical functions in any effective corporate anti-virus process. This could be mitigated if there was some mechanism for displaying tailored messages (as is now supported with DOEVStop), but only the Windows scanner can support targeted messaging.

The second is significant voids in addressing macro viruses. However, the ASSIST's expertise in this area provides the capability of addressing this problem through program augmentation, which should be sufficient for the near future. However, it is hoped that Norman develops a viable real-time detection capability for this class of viruses so that DOEVMon maintenance can be curtailed.